CLAIMS

1.   (Currently Amended) An optical data storage medium comprising:

a memory;

one or more processors operatively coupled to the memory and disposed within one or more devices;

optically-readable material suitable for storing data therein; [[and]]

stored within said optically-readable material, instructional data for an optical media content protection scheme, said instructional data being configured to cause logic associated with an optical media receiving device to operatively perform in accordance with said optical media content protection scheme when programmed using said instructional data and accessing associated content data stored on said optical data storage medium,

at least one optically-detectable authentication component,

wherein said at least one optically-detectable authentication component includes a plurality of optically-detectable authentication components forming a substantially unique pattern using at least one optically detectable material,

wherein said optically detectable material includes at least one material selected from a group of optically detectable materials comprising an opaque material, a partially opaque material, a polymer-based material, and an epoxy-based material,

wherein said at least one optically-detectable authentication component forms an optically-detectable certificate of authentication (COA);

stored within said optically-readable material, COA information data, said COA information data including at least one type of data associated with said COA selected

from a group of COA information data comprising raw optically-detected COA data, COA related plaintext data, and COA related signature data; and

at least one top surface material, wherein said at least one optically-detectable authentication component is formed on said top surface material.

2.   (Original) The optical data storage medium as recited in Claim 1, wherein said optical media content protection scheme includes a digital rights management (DRM) protection scheme.

3.   (Original) The optical data storage medium as recited in Claim 2, wherein said DRM protection scheme includes at least one marking scheme selected from a group of marking schemes comprising a data-implemented water marking scheme and a data-implemented forensic marking scheme.

4.   (Currently Amended) The optical data storage medium as recited in Claim 1, further comprising at least one type of additional data stored within said optically-readable material, wherein said type of additional data being is selected from a group of additional data comprising substantially unique identifier data associated with said optical data storage medium, licensing data associated with said optical data storage medium, and said content data.

5.   (Canceled)

6.   (Canceled)

Serial No.: 10/706,305
Atty Docket No.: MS1-1659US
Atty/Agent: Dale G. Mohlenhoff
-3-   lee&hayes The Business of IP®
www.leehayes.com • 509.324.9256

7.   (Canceled)

8.   (Canceled)

9.   (Canceled)

10.   (Canceled)

11.   (Currently Amended) The optical data storage medium as recited in Claim [[5]] 1, further comprising:

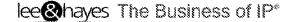at least one top surface material and wherein at least one of the following occurs:

said at least one optically-detectable authentication feature is formed on said top surface material;

said at least one optically-detectable authentication feature component is formed below said top surface material; and

said at least one optically-detectable authentication feature component extends at least partially into said top surface material.

12.-17   (Canceled)

18.   (Currently Amended) An apparatus comprising:

a memory;

one or more processors operatively coupled to the memory and disposed within one or more devices;

means for storing instructional data for an optical media content protection scheme within an optical data storage medium, said instructional data being configured to cause logic associated with an optical media receiving device to operate in accordance with said optical media content protection scheme when programmed using said instructional data and accessing associated content data stored on said optical data storage medium;

means for causing at least one optically-detectable authentication component to be included in said optical data storage medium, wherein said optically-detectable authentication component includes a plurality optically-detectable authentication components forming a substantially unique pattern using at least one optically detectable material, wherein said at least one optically-detectable authentication component forms an optically-detectable certificate of authentication (COA), wherein said optically detectable material includes at least one material selected from a group of optically detectable materials comprising an opaque material, a partially opaque material, a polymer-based material, and an epoxy-based material;

means for storing COA information data within said optical data storage medium and

means for generating said COA information data, wherein said COA information data includes at least one type of data associated with said COA selected from a group of COA information data comprising raw optically-detected COA data, COA related plaintext data, and COA related signature data; and

means for at least one top surface material, wherein said at least one optically-detectable authentication component is formed on said top surface material.

19.   (Original) The apparatus as recited in Claim 18, wherein said optical media content protection scheme includes a digital rights management (DRM) protection scheme.

20.   (Original) The apparatus as recited in Claim 19, wherein said DRM protection scheme includes at least one marking scheme selected from a group of marking schemes comprising a data-implemented water marking scheme and a data-implemented forensic marking scheme.

21.   (Original) The apparatus as recited in Claim 18, further comprising:
means for storing at least one type of additional data within said optical data storage medium, said type of additional data being selected from a group of additional data comprising substantially unique identifier data associated with said optical data storage medium, licensing data associated with said optical data storage medium, and said content data.

22.   (Canceled)

23.   (Canceled)

24.   (Canceled)

Serial No.: 10/706,305
Atty Docket No.: MS1-1659US
Atty/Agent: Dale G. Mohlenhoff
-6-
lee&hayes The Business of IP®
www.leehayes.com ● 509.324.9256

25.   (Canceled)

26.   (Canceled)

27.   (Canceled)

28.   (Canceled)

29.   (Currently Amended) The apparatus as recited in Claim [[22]] 18,

further comprising:

wherein said optical data storage medium includes at least one top surface

material, and further comprising at least one means for causing at least one of the

following functions to occur:

forming said at least one optically-detectable authentication feature on

said top surface material;

forming at least one optically-detectable authentication feature

component below said top surface material; and

forming said at least one optically-detectable authentication feature

component such that said at least one optically-detectable authentication feature

component extends at least partially into said top surface material.

30.-35.   (Canceled)

36.   (Currently Amended) An apparatus comprising:

a memory;

one or more processors operatively coupled to the memory and disposed within one or more devices;

a data storage device configurable to write data to an optical data storage medium; and

logic operatively coupled to said configured to said data storage device and configured to cause said data storage device to record instructional data for an optical media content protection scheme within said optical data storage medium, said instructional data being configured to cause logic associated with an optical media receiving device to operate in accordance with said optical media content protection scheme when programmed using said instructional data and accessing associated content on said an optical data storage medium,

wherein said optical data storage medium further includes a plurality of optically-detectable authentication components forming a substantially unique pattern using at least one optically detectable material and an optically-detectable certificate of authentication (COA),

wherein said optically detectable material includes at least one material selected from a group of optically detectable materials comprising an opaque material, a partially opaque material, a polymer-based material, and an epoxy-based material,

wherein said logic is further configured to cause said data storage device to record COA information data within said optical data storage medium,

wherein said COA information data includes at least one type of data associated with said COA selected from a group of COA information data comprising raw optically-detected COA data, COA related plaintext data, and COA related signature data; and

at least one top surface material, wherein said at least one optically-detectable authentication component is formed on said top surface material.

37.   (Original) The apparatus as recited in Claim 36, wherein said optical media content protection scheme includes digital rights management (DRM) protection scheme.

38.   (Original) The apparatus as recited in Claim 37, wherein said DRM protection scheme includes at least one marking scheme selected from a group of marking schemes comprising a data-implemented water marking scheme and a data-implemented forensic marking scheme.

39.   (Original) The apparatus as recited in Claim 36, wherein said logic is further configured to cause said data storage device to record at least one type of additional data within said optical data storage medium, said type of additional data being selected from a group of additional data comprising substantially unique identifier data associated with said optical data storage medium, licensing data associated with said optical data storage medium, and content data.

40.   (Canceled)

41.   (Currently Amended) The apparatus as recited in Claim [[40]] 36, wherein said data storage device is further configurable to detect said at least one optically-detectable authentication ~~feature~~ component and provide resulting authentication ~~feature~~ component information to said logic.

42.   (Canceled)

43.   (Canceled)

44.   (Canceled)

45.   (Canceled)

46.-48.   (Canceled)

49.   (Currently Amended) One or more computer readable media storing computer-executable instructions that, when executed, perform a [[A]] method comprising:

storing instructional data for an optical media content protection scheme within an optical data storage medium, said instructional data being configured to cause logic associated with an optical media receiving device to operate in accordance with said optical media content protection scheme when programmed using said instructional data and accessing associated content data stored on said optical data storage medium;

causing at least one optically-detectable authentication component to be included in said optical data storage medium, wherein said optically-detectable authentication component includes a plurality of optically-detectable authentication components forming a substantially unique pattern using at least one optically detectable material,

wherein said plurality of optically-detectable authentication components includes at least one optically-detectable authentication component forming a substantially unique pattern using at least one optically detectable material,

wherein said optically detectable material includes at least one material selected from a group of optically detectable materials comprising an opaque material, a partially opaque material, a polymer-based material, and an epoxy-based material,

wherein said at least one optically-detectable authentication component forms an optically-detectable certificate of authentication (COA);

storing COA information data within said optical data storage medium, wherein said COA information data includes at least one type of data associated with said COA selected from a group of COA information data comprising raw optically-detected COA data, COA related plaintext data, and COA related signature data; and

generating said COA information data.

50.   (Original) The method as recited in Claim 49, wherein said optical media content protection scheme includes a digital rights management (DRM) protection scheme.

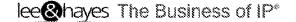51.   (Original) The method as recited in Claim 50, wherein said DRM protection scheme includes at least one marking scheme selected from a group of

marking schemes comprising a data-implemented water marking scheme and a data-implemented forensic marking scheme.

52.   (Original) The method as recited in Claim 49, further comprising:

storing at least one type of additional data within said optical data storage medium, said type of additional data being selected from a group of additional data comprising substantially unique identifier data associated with said optical data storage medium, licensing data associated with said optical data storage medium, and said content data.

53.   (Canceled)

54.   (Canceled)

55.   (Canceled)

56.   (Canceled)

57.   (Canceled)

58.   (Canceled)

59.   (Canceled)

60.　　　　(Currently Amended) The method as recited in Claim [[53]] 49, further comprising:

wherein said optical data storage medium includes at least one top surface material, causing at least one of the following acts to occur:

~~forming said at least one optically-detectable authentication feature on said top surface material;~~

forming at least one optically-detectable authentication ~~feature~~ component below said top surface material; and

forming said at least one optically-detectable authentication ~~feature~~ component such that said optically-detectable authentication ~~feature~~ component extends at least partially into said top surface material.

61.-66.　　(Canceled)

67.　　　　(Currently Amended) A computer-readable medium storing ~~comprising~~ computer-implementable instructions for causing at least one processor to perform acts comprising:

writing instructional data for an optical media content protection scheme to an optical data storage medium, said instructional data being configured to cause logic associated with an optical media receiving device to operate in accordance with said optical media content protection scheme when programmed using said instructional data and accessing associated content data stored on said optical data storage medium, wherein said optical data storage medium further includes at least one optically-detectable authentication component;

wherein said optical data storage medium further includes at least one optically-detectable authentication component forming a substantially unique pattern using at least one optically detectable material and an optically-detectable certificate of authentication (COA),

wherein said optically detectable material includes at least one material selected from a group of optically detectable materials comprising an opaque material, a partially opaque material, a polymer-based material, and an epoxy-based material,

wherein said logic is further configured to cause said data storage device to record COA information data within said optical data storage medium,

wherein said COA information data includes at least one type of data associated with said COA selected from a group of COA information data comprising raw optically-detected COA data, COA related plaintext data, and COA related signature data;

at least one top surface material, wherein said at least one optically-detectable authentication component is formed on said top surface material writing COA information data to said optical data storage medium, wherein said COA information data includes at least one type of data associated with said COA selected from a group of COA information data comprising raw optically-detected COA data, COA related plaintext data, and COA related signature data; and

generating said COA information data.

68.   (Original) The computer-readable medium as recited in Claim 67, wherein said optical media content protection scheme includes a digital rights management (DRM) protection scheme.

69.   (Original) The computer-readable medium as recited in Claim 68, wherein said DRM protection scheme includes at least one marking scheme selected from a group of marking schemes comprising a data-implemented water marking scheme and a data-implemented forensic marking scheme.

70.   (Original) The computer-readable medium as recited in Claim 67, further comprising:

writing at least one type of additional data to said optical data storage medium, said type of additional data being selected from a group of additional data comprising substantially unique identifier data associated with said optical data storage medium, licensing data associated with said optical data storage medium, and said content data.

71.   (Canceled)

72.   (Canceled)

73.   (Canceled)

74.   (Canceled)

75.   (Currently Amended) An apparatus, comprising:

non-volatile memory;

an interface mechanism suitable for receiving a removable optical data storage medium, accessing instructional data associated with an optical media content

protection scheme from said optical data storage medium, and outputting said accessed instructional data;

logic operatively coupled to said interface mechanism and said non-volatile memory and configured to receive said accessed instructional data and in response thereto update a current optical media content protection scheme stored in said non-volatile memory and thereafter while accessing associated content data stored on said optical data storage medium operatively adhere to said updated current optical media content protection scheme,

wherein said interface mechanism is further configured to detect at least one optically-detectable authentication component that is part of said optical data storage medium and output corresponding information to said logic,

wherein said optical data storage medium further includes at least one optically-detectable authentication component forming a substantially unique pattern using at least one optically detectable material and an optically-detectable certificate of authentication (COA),

wherein said interface mechanism is further configured to access COA information data stored within said optical data storage medium and provide said COA information data to said logic,

wherein said optically detectable material includes at least one material selected from a group of optically detectable materials comprising an opaque material, a partially opaque material, a polymer-based material, and an epoxy-based material,

wherein said logic is further configured to cause said data storage device to record COA information data within said optical data storage medium,

wherein said COA information data includes at least one type of data associated with said COA selected from a group of COA information data comprising raw optically-detected COA data, COA related plaintext data, and COA related signature data;

at least one top surface material, wherein said at least one optically-detectable authentication component is formed on said top surface material,

wherein said logic is further configured to verify said COA information data, and is configured to update said current optical media content protection scheme stored in said non-volatile memory once said COA information data has been verified.

76.   (Original) The apparatus as recited in Claim 75, wherein said current optical media content protection scheme causes said logic to adhere to a digital rights management (DRM) protection scheme.

77.   (Original) The apparatus as recited in Claim 76, wherein said DRM protection scheme includes at least one marking scheme selected from a group of marking schemes comprising a data-implemented water marking scheme and a data-implemented forensic marking scheme.

78.   (Original) The apparatus as recited in Claim 75, wherein said interface mechanism is further configured to access and output to said logic at least one type of additional data stored on said optical data storage medium, said type of additional data being selected from a group of additional data comprising substantially unique identifier data associated with said optical data storage medium, licensing data associated with said optical data storage medium, and said content data.

79.   (Canceled)

80.   (Canceled)

81.   (Canceled)

82.   (Canceled)

83.   (Canceled)

84.   (Canceled)

85.   (Currently Amended) The apparatus as recited in Claim [[84]] 75, wherein said interface mechanism is further configured to access license information data stored within said optical data storage medium and provide said license information data to said logic, and wherein said logic is configured to verify said license information data to determine if content data stored on said optical data storage medium can be accessed.

86.   The apparatus as recited in Claim 85, wherein said logic maintains license usage information within said non-volatile memory.

87.-104.   (Canceled)